Saimaa University of Applied Sciences
Faculty of Technology Lappeenranta
Double Degree
Information Technology

Tarek Batiha

Network Analysis for the Industrial Company

Thesis 2014

Abstract

Tarek Batiha
Network Analysis for the Industrial Company, 35 pages
Saimaa University of Applied Sciences
Faculty of Technology, Lappeenranta
Double Degree
Information Technology
Thesis 2014
Instructor: Lecturer Yrjö Utti, Saimaa University of Applied Sciences

The main purpose of this thesis was to analyze the network environment of the MPS Mont company, then based on the analysis to offer some improvements. Another important goal was to get knowledge of processes in a real company.

The improvements in the network environment had to be without any expenditures for the company. The solution was based on opensource software.

The final result of this thesis was documentation of the company's network and deployment of a honeypot based on opensource system honeyd.

Keywords: Network, OSI, honeypot

List of terms

AES – Advanced Encryption Standard – symmetric-key cryptosystem.

CRC – Cyclic Redundancy Check - an error-detecting code commonly used in digital networks and storage devices to detect accidental changes to raw data (“Cyclic redundancy check - Wikipedia, the free encyclopedia,” n.d.)

DNS – Domain Name System - is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network (“Domain Name System - Wikipedia, the free encyclopedia,” n.d.).

FTP – File Transfer Protocol - a standard network protocol used to transfer files from one host to another host over a TCP-based network, such as the Internet (“File Transfer Protocol - Wikipedia, the free encyclopedia,” n.d.).

GNU – GNU's not Unix – UNIX like operating system respecting freedom

GPL – GNU General Public License - the most widely used[5] free software license, which guarantees end users (individuals, organizations, companies) the freedoms to use, study, share (copy), and modify the software (“GNU General Public License - Wikipedia, the free encyclopedia,” n.d.).

GUI – Graphic User Interface

HPC – High-erformance Computing – computing on supercomputers.

HTML - HyperText Markup Language – language used to create web pages.

HTTP – Hypertext Transfer Protocol – communication protocol used for accessing web pages.

HTTPS – Hypertext Transfer Protocol Secure – HTTP secured by SSL or TLS.

IEEE - Institute of Electrical and Electronics Engineers

IP - Internet Protocol – is the principal communications protocol in the Internet protocol suite for relaying datagrams across network boundaries (“Internet Protocol - Wikipedia, the free encyclopedia,” n.d.)

IPv4 – Internet Protocol version 4 – IP fourth version.

IPv6 - Internet Protocol version 6 - IP sixth version.

ISO - International Organization for Standardization - an international standard-setting body composed of representatives from various national standards organizations (“International Organization for Standardization - Wikipedia, the free encyclopedia,” n.d.).

LAN – Local Area Network -network of devices connected in restricted area like school or building.

MD5 – Message-digest Algorithm – cryptographic hash function.

NAT – Network Address Translation – method of translating private IP addresses to public.

OS – Operating System – a layer between commuter hardware and running programs acceding the hardware through operating system.

OSI - Open Systems Interconnection – seven layered model describing communication between network devices.

PC – Personal Computer

PDU – Protocol Data Unit -Information that is delivered as a unit among peer entities of a network and that may contain control information, such as address information, or user data (“Protocol data unit - Wikipedia, the free encyclopedia,” n.d.).

POP3 – Post Office Protocol – protocol designed to download email from server through TCP/IP protocol.

POSIX - Portable Operating System Interface

RSA - Rivest, Shamir, Adleman – public-key cryptosystem

SFTP – SSH File Transfer Protocol – normal FTP protocol secured by SSH

SMNP – Simple Network Management Protocol – an Internet-standard protocol for managing devices on IP networks (“Simple Network Management Protocol - Wikipedia, the free encyclopedia,” n.d.).

SMTP -Simple Mail Transfer Protocol – Internet protocol designed to send and receive emails.

SQL - Structured Query Language - a special-purpose programming language designed for managing data held in a relational database management system (“SQL - Wikipedia, the free encyclopedia,” n.d.)

SSH -Secure Shell – cryptographic network protocol for securing data communication.

SSL – Secure Socket Layer – cryptographic protocol providing communication security over Internet.

TCP – Transmission Control Protocol - provides reliable, ordered and error-checked delivery of a stream of octets between programs (“Transmission Control Protocol - Wikipedia, the free encyclopedia,” n.d.)

TLS – Transport Layer Security - cryptographic protocol providing communication security over Internet.

UDP – User Datagram Protocol - computer applications can send messages, in this case referred to as *datagrams*, to other hosts on an Internet Protocol (IP)

network without prior communications to set up special transmission channels or data paths (“UDP - Wikipedia, the free encyclopedia,” n.d.).

UTP - Unshielded Twisted Pair – type of cable used in local area networks.

ARP - Address Resolution Protocol (ARP) is a telecommunication protocol used for resolution of network layer addresses into link layer addresses, a critical function in multiple-access networks (“Address Resolution Protocol - Wikipedia, the free encyclopedia,” n.d.).

DHCP - Dynamic Host Configuration Protocol - a standardized networking protocol used on Internet Protocol (IP) networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services. With DHCP computers request IP addresses and networking parameters automatically from a DHCP server, reducing the need for a network administrator or a user to configure these settings manually (“Dynamic Host Configuration Protocol - Wikipedia, the free encyclopedia,” n.d.).

CPU – Central Processing Unit – basic component of computer.

MAC - Media Access Control - an address (MAC address) is a unique identifier assigned to network interfaces for communications on the physical network segment (“MAC address - Wikipedia, the free encyclopedia,” n.d.).

Table of Contents

1. Introduction

Network environment is nowadays a very important part of basically every company without difference of focus. It defines interconnection between devices like personal computers and printers which are important for accounting in some small company to interconnect thousands of servers in a data center run by a company providing cloud services on the Internet.

The main goal of this thesis was to analyze such an environment in a mid-sized industrial company. The analysis consisted of a condition assessment and then to offer what could be improved based on the analysis.

Chapter two briefly describes the company in which the work was made.

In chapter 3 the specifics of the analysis are mentioned . In this chapter the reader can find the main goals of the thesis.

In chapter 4 some important theoretical knowledge is mentioned. This knowledge was an important part of the network analysis, necessary to make the work right.

Chapter 5 describes the results of the work with emphasis on the technical part of the work. There are described details of the results of the analysis.

Finally chapter 6 is the conclusion. In this chapter you can read what this thesis gave to the author.

2. About the company

With the more than 20 years of tradition in production and installation operations, the company belongs to traditional suppliers in power industry, combined heat and power production and petrochemistry.

MPS Mont a.s. (a.s. means stock company in Czech language) procures comprehensive supplies for construction, upgrades, renovation and maintenance within a broad spectrum of industrial sectors, especially combined heat and power production, petrochemistry, power engineering, mechanical engineering and food industry.

The company's services include project development and supply of machinery and electrotechnical units, their servicing, maintenance, general overhauls and

after warranty servicing (“Company | MPS Mont a.s.,” n.d.).In figure 1 you can see entrance to the area.

Figure 1. Entrance to the company

3. Analysis

This chapter is describes the analysis of the company's network environment.

3.1 Current state

The task at the MPS company was to analyze the network environment, to analyze the current state and based on the analysis, to offer some improvements. The improvements should make the network more efficient and reliable in future.

The first step in this task was to check out the documentation of the network and make a decision based on that. Unfortunately there was not appropriate documentation. So the first task was to walk through all offices and draw all the elements of the network and how are they connected. Another problem was that there are no labels at the UTP (Unshielded Twisted Pair) sockets in the wall. The next situation was that some employees objected that their network connection is not working properly.

So the task was to analyze all these problems and find a solution to them, and if possible to make some improvements in the network.

3.2 Improvements

So the solution was split into to three parts. The first part was to make network environment documentation and design UTP naming system. The documentation had to be complex but easy to understand. The next task was to check all the network interfaces reliability. In this task any tools which would mean expenditures for the company would not be used. And the final task was to design some improvement in the company's network environment. To increase cyber security in the company's network environment honeypot, a system based on open source software was designed.

4. Theory

This section describes some technologies and principles of network protocols. This knowledge is necessary to understand the network environment and then to provide work results on high level.

4.1 ISO/OSI model

Open Systems Interconnection model (OSI) is a conceptual model that standardizes the functions of communication system by dividing it to the abstraction layers - see figure 2. It was created by ISO (International Organization for Standardization) organization and in 1984 accepted as international standard ISO 7498 (“OSI model - Wikipedia, the free encyclopedia,” n.d.).

The model splits the communication functions into seven layers. The OSI is not only one model, there is for example a TCP/IP(transmission control Protocol/Internet Protocol) model , which has only four layers - differences in figure 2. The layers of OSI model are abstract so the norm does not specify the realization or implementation of the systems, but describes only the general principles of seven layered network architecture.

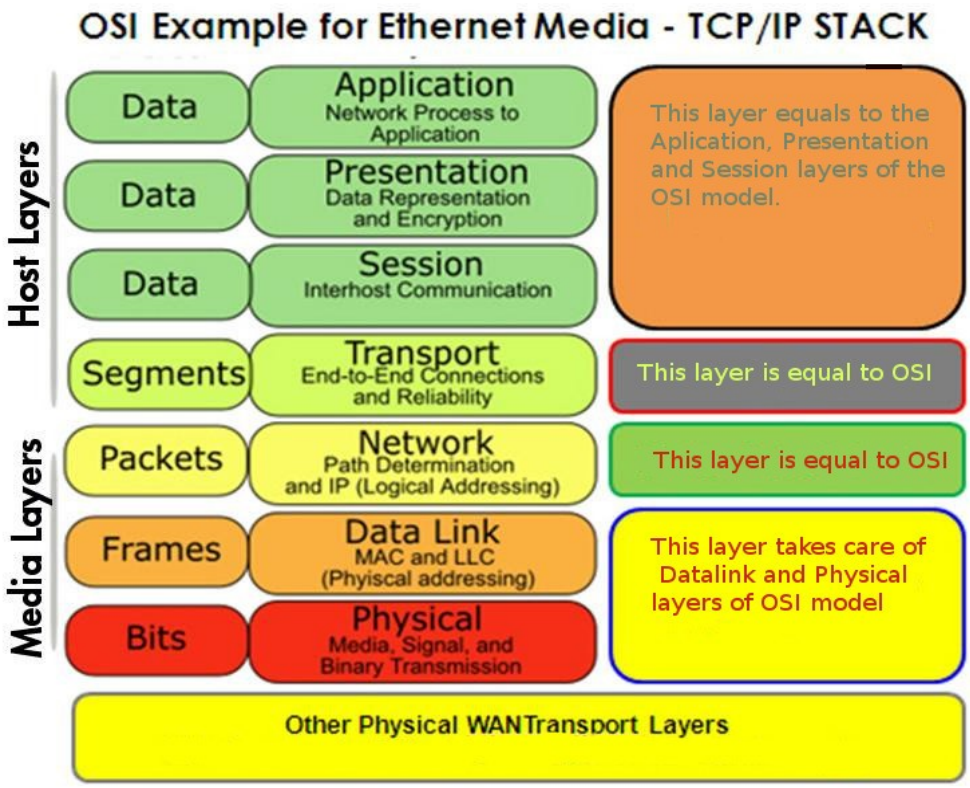

Figure 2. Osi model vs TCP/IP model

It describes the functions and services on the layers. The unit of one OSI layer is called PDU (protocol data unit). PDU is specified by protocol of the layer and may contain various information, which are protocol specific . See Figure 3 – example of two different layer PDUs.

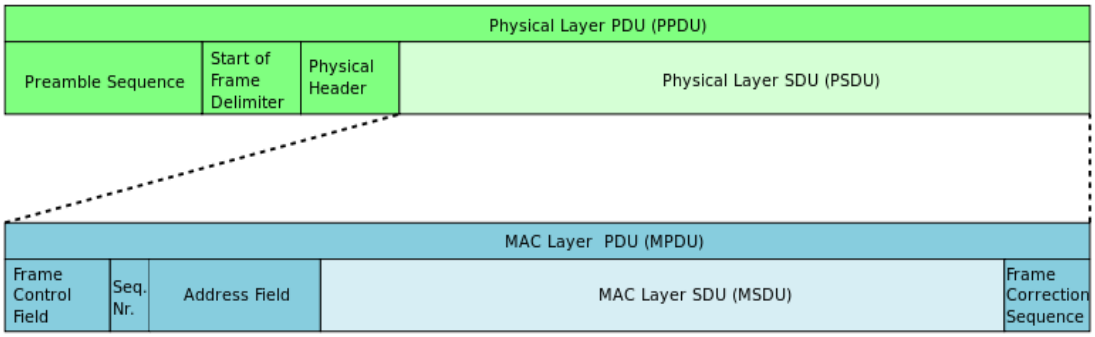

Figure 3. PDU

4.1.1 Layer 1 – physical layer

The physical layer is the first layer of the OSI model. It provides transfer of a bit stream to signal (usually electric) and reverse, transfer of the signal to the stream of bits (“Physical layer - Wikipedia, the free encyclopedia,” n.d.).

Protocols of physical layer specify electrical properties of interface like voltage or line impedance and also mechanical properties – for example copper of fiber optical cable .

The realization of this layer is on hardware level, because it works directly with signal. The example of a device that works only on physical layer is hub. This device is designed co connect devices on network, for example to interconnect few PCs (Personal Computer). When one PC is trying to communicate with an other it sends data in the form of an electric signal to the hub. Because the hub works only on physical layer it cannot determine where to send the data because there are no addresses or such information on physical layer . The hub then sends the data to all its interfaces and all PCs connected to the hub to receive the same data, except the PC which sends them. This is a very noneffective and insecure way of communication so nowadays this device is practically not used.

4.1.2 Layer 2 – data link layer

Data link layer is the second layer of OSI model. It provides a reliable connection between two connected nodes. It also provides error detection. The PDU of this layer is called frame (“Data link layer - Wikipedia, the free encyclopedia,” n.d.).

The main features of data link layer:

- physical addressing
- media access control
- is hardware independent

Data link layer receives a packet from the network layer. Then add some additional data to the packet and this unit creates a frame. Typical added information are physical address from the receiver and the sender, start and end of the frame or type of the message. Before the frame is sent, CRC (Cyclic Redundancy Check) sum of the frame is counted and then the result is added to the frame. When frame is received by the receiving host, CRC is counted again and if it is not equal to the value counted by the sender, the frame is dropped.

A typical device of data link layer is switch. This device is designed to work on the layer 2 of OSI model. It connects two or more devices on the same LAN (Local Area Network). So it means that the switch works with frames. When a frame is received it is forwarded to the specific interface based on hardware address which is located in the frame. This is very fast and efficient so this device is nowadays replaced by hubs. Actually it is the fastest way of network communication nowadays, so for example in data centers or cloud devices are interconnected by switches because of their requirements for high speed and low latency.

4.1.3 Layer 3 – network layer

Network layer is the third layer of OSI model. The layer provides exchange of data between end devices through network – so called end-to-end communication. PDU of this layer is called packet (“Network layer - Wikipedia, the free encyclopedia,” n.d.).

The main functions of network layer:

- connectionless communication
- host addressing
- message forwarding

End devices in network have attached unique network address. The device with these address is called host. Network addresses are designed to route packets through network and for unique host identification on the Internet.

The form of address could be in different versions of IP protocol. Today the most used protocol is IPv4 (Internet Protocol version 4) with address format x.x.x.x where x is representing an 8 bit number. But nowadays the IPv4 address range is no longer applicable. It is because there is limit of addresses and all network ranges have already been assigned. So it means that only organizations that had assigned any range already, have some addresses left. Now Internet is slowly starting to use IPv6 (Internet Protocol Version 6) addresses. IPv6 limit of network addresses is because it uses 128 bit addresses. It is very likely that in distant future IPv6 address range will not be wasted.

IPv4 addresses

Important thing in IPv4 is network range. Network range determines how many hosts there could be in the network. It is given by *network mask.* Mask is usually written in decimal format or in form of IP address. If it is written in decimal format, it is the number which represents the count of bits which are 1 from left to right. Others are 0. So for example mask /24 will be in address format 255.255.255.0, in binary representation it is 1111111.11111111.11111111.00000000 – we can count 24 occurrences of 1. The binary negation of mask then means how many hosts there are available in the network range. In this case we can see it is thus 256 addresses, but the first address is network and the last broadcast address. The result is then 254 host addresses.

There are some special addresses which the host cannot have. The first is 127.0.0.1/8. This address range is called *localhost*. It is used for loopback purposes. There are private address ranges. It means that these addresses cannot be accessed from the Internet. The purpose of private addresses is for networks not connected to the Internet or for NAT (Network Address Translation). Network Address Translation is used when an organization has more devices that need Internet access than the count of available public addresses.

The list of private address ranges:

- 10.0.0.0/8

- 172.16.0.0/12
- 192.168.0.0/16

Addresses that also cannot be used as host addresses are network and broadcast address. Network address is always the first address in network range and broadcast is the last. We can get network mask by logical AND of IP (Internet Protocol) address and network mask. These addresses are used for routing and broadcasting purposes.

An example of network and broadcast address for network 192.168.0.0/16:

- Network - 192.168.0.0
- Broadcast – 192.168.255.255

4.1.4 Layer 4 - transport layer

The transport layer is the fourth layer of OSI model. The purpose of this layer is to identify communication of specified application and to forward data to a specific application (“Transport layer - Wikipedia, the free encyclopedia,” n.d.).

The main features of transport layer:

- Segmentation
- Reassembling
- Identification of application
- Multiplexing
- Encapsulation

The transport layer before sending, segments data flow from application and then, after receiving, reassembles it back. Addressing on this layer is made by port numbers which represent communicating applications.

Port number

Port number is a 16 bit number thus it is in range 0 – 65536. It is always placed in the header of segment or the datagram of transport layer. The port number is united with remote application so the client application must know port number if it wants to connect to this application. The ports in range 0 – 1023 are fixed and well-known for clients (“Port (computer networking) - Wikipedia, the free encyclopedia,” n.d.).

Examples of well known ports:

- *20 & 21*: FTP (File Transfer Protocol)
- *22*: SSH (Secure Shell)
- *23*: Telnet
- *25*: SMTP (Simple Mail Transfer Protocol)
- *53*: DNS (Domain Name System)
- *80*: HTTP (Hypertext Transfer Protocol)
- *110*: POP3 (Post Office Protocol)
- *443*: HTTPS (Hypertext Transfer Protocol Secure)

There are many protocols on transport layer but the best known are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol). TCP is more reliable than UDP but requires more moderation. So these protocols fit differently to different situations. Both will be explained later.

4.1.5 Layers 5,6,7

These layers are not so important for the thesis so they will be mentioned briefly.

Layer 5 – session layer

This layer organizes and synchronizes the dialogue between session layers of cooperating systems and controls data exchange between them. An example of protocol working on this layer is SSL (Secure Sockets Layer).

Layer 6 – presentation layer

The purpose of this layer is to transform data to the form with which the application is working. Examples of functions of presentation layer are code or alphabet conversion.

Layer 7 – application layer

The purpose of this layer is to give access to applications to the communicating system and allow them to cooperate. Examples of protocols running on this layer are FTP, DNS, POP3 and more.

4.2 TCP

TCP (Transmission Control Protocol) is one of the basic protocols on the Internet. It works on the transport layer of the OSI model, which is described in detail in chapter 3.1.4.

TCP is a connection-oriented protocol. From this property result some of its advantages. The connection is established before the data is sent. It creates virtual connection between two hosts so the sender knows that the host is reachable before sending data. TCP segments data flow to the segments - so-called packets. The packets have their own sequence number – a number which represents the order of packets. The packets are sent through virtual circuit – this means that data could be sent through different paths in the Internet – because of better scalability. After receiving packets, TCP reassembles them to the original data flow.

Three way handshake

The connection between two hosts is established in a so-called three way handshake. It is for hosts to agree on SYN and ACK flags.

Handshake:

- Client sends to server SYN with random generated sequence number and acknowledgement number which equals 0.
- Server responds with SYN ACK. Sequence number is incremented by 1 and acknowledgement number is randomly generated.
- Client responds with ACK, sequence and acknowledgement numbers are both incremented by 1.

Both sides then remember their sequence numbers. They are used to the next communication. The connection is established until one of the sides terminate it. In Figure 4 you can see the graphical example.

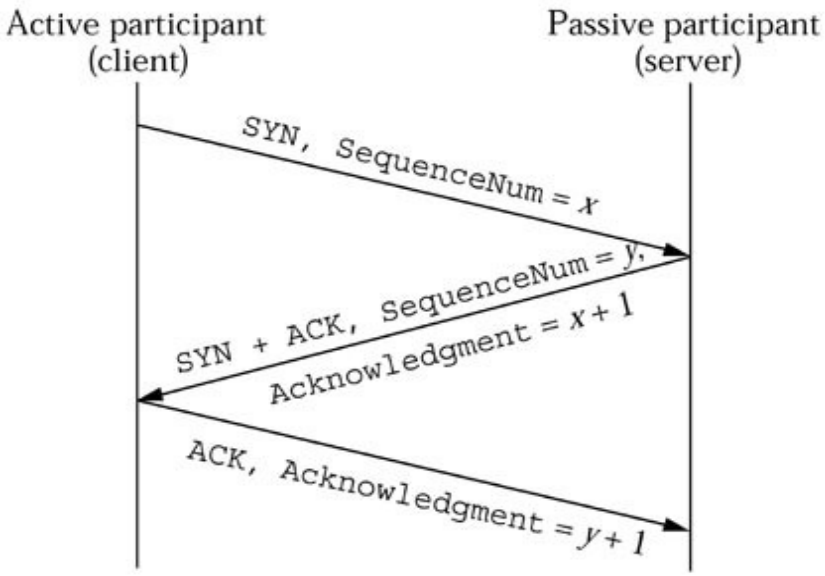

Figure 4. Three-way handshake

Terminating connection

To terminate connection the client sends FIN to the server. Then the server responds with ACK. Then servers send FIN. The client responds with ACK. After these four steps connection is terminated.

4.3 UDP

UDP (User Datagram Protocol) is the protocol of the fourth layer of OSI model. UDP is not connection-oriented and sometimes is is marked as unreliable (“UDP - Wikipedia, the free encyclopedia,” n.d.).

User datagram protocol works very simply. It just sends a packet through the network. UDP protocol does not concern if the host is reachable. It sends datagrams without segmenting them to packets. The PDU is then called a datagram. It does not give any sequence number or such things so data could arrive to the host out of order. The datagram could also be lost somewhere on the network but all this are attributes of UDP. Figure 5 are displays different properties between TCP and UDP protocols.

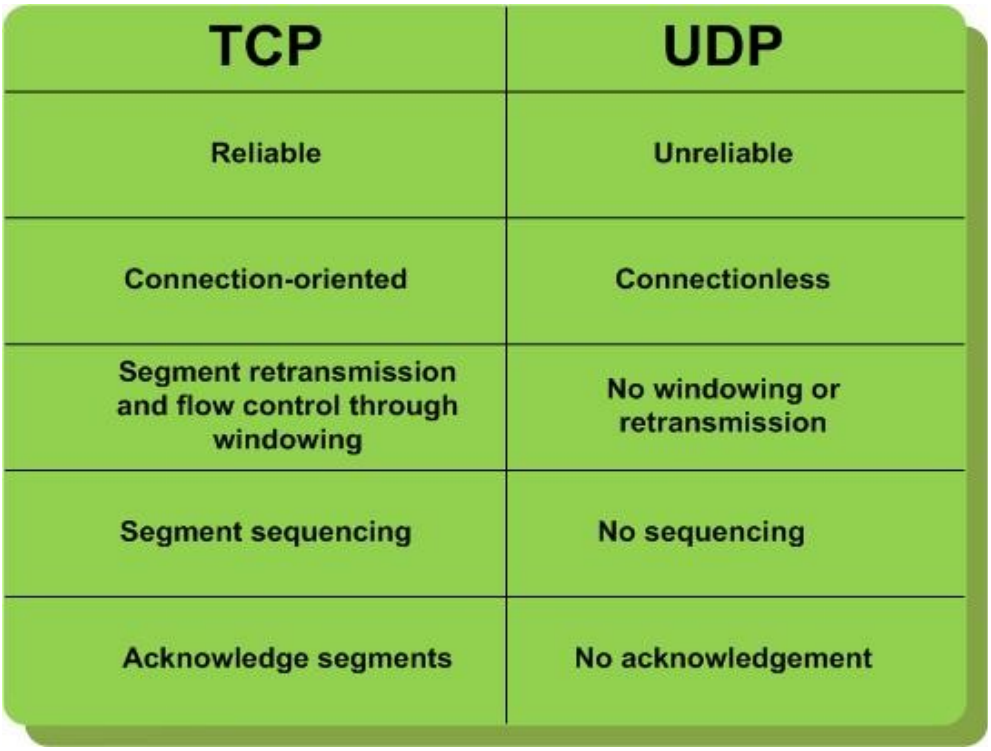

Figure 5. UDP vs TCP

On the other hand UPD is not consuming so much system resources as TCP. It is appropriate to use UDP in situations where its disadvantages are not a problem, but the user can gain from its simplicity. An example is DNS server which works on question answer principle. The server saves system resources because it is not establishing connections and has faster response time. The

network bandwidth is also reduced. The next example is VoIP (Voice over IP) or video streaming. In such situations it is not a problem if some datagrams are lost on the network, because in conversation or in video call a human will not notice such a small loss. It also supports multicast and broadcast technologies which is very useful in live video streaming.

4.4 Well known services

This chapter briefly describes some of the well-known services running on the most operating systems. Described are services which were used in the work for the company.

4.4.1 Telnet

Telnet is a shortcut from telecommunication network. It is a protocol which allows the user to connect to a remote host. Telnet is working on application layer of OSI model. It is client-server oriented and it uses TCP protocol and usually works on port 23. It was used as a remote terminal in the past, but nowadays not anymore, because telnet does not use any encryption. Its only plain text. It is used for debugging applications or services.

4.4.2 SSH

SSH (Secure Shell) is a network protocol using TCP/IP. It was designed as a replacement for telnet and other remote shells because of theirs lack of encryption. SSH is commonly listening on port 22. It is used as a remote terminal or any form of secured data transmission.

4.4.3 HTTP

HTTP (Hyper Text Transfer Protocol) is a well-known Internet protocol designed for exchange of hypertext documents in HTML (HyperText Markup Language) format. It works on application layer of OSI model. HTTP does not include any kind of encryption or data integrity check. It uses TCP/IP and is usually using port 80. HTTP works as question-answer in which the client sends a plain text

question containing data about the requested document and some additional information. The server then responses with an answer in the form of answer to question followed by the requested document.

4.4.4 FTP

FTP (File Transfer Protocol) is a protocol designed to transfer files through network. It works on application layer of OSI model and it usually uses ports 20 and 21. Port 21 is using server for exchanging messages with the client. Data is sent on port 20 and while sending files communication on port 21 is empty. This is a problem if there is a firewall running, because it might block port 21. This version does not support encryption but there is a secured version – SFTP (Secure File Transfer Protocol). It is commonly used to transfer music, video etc.

4.4.5 POP3

POP3 (Post Office Protocol) is a protocol designed to download emails from server to client. It works on application layer of OSI model. Port 110 is commonly used for this protocol. POP3 is unencrypted but there are some clients which support MD5 (Message-digest Algorithm) hashed passwords or encrypting the whole communication with SSL (Secure Sockets Layer) or TLS (Transport Layer Security).

4.5 GNU General Public License

GPL is a license for free software originally written by Richard Stallman of the Free Software Foundation for GNU project. GPL is a well-known example of a strong copyleft license. Copyleft means that the derived version of work (some software etc.) must be published by the same license as original.

GNU guarantees the recipients of computer program the rights of Free Software Definition and use copyleft to guarantee that freedom is always prevented.

Any company can use GPL licensed software for internal use for free. Only if the source code would be modified a new source code must be published by GPL.

5. Used tools

This chapter describes tools which were used during the development.

5.1 Microsoft Visio

Microsoft Visio is an application for diagramming and vector graphics. It is part of Microsoft Office suite. It was first introduced in 1992 by Shapeware corporation but in 2000 it was acquired by Microsoft.

5.2 Virtualbox

Oracle VM VirtalBox is a virtualization software for x86 or AMD64/Intel64 based systems. This tool is a multi platform thus it supports multiple operating systems. Virtalbox was originally developed by a German company GmbH but in 2008 the company was bought by Sun Microsystems. In 2009 Sun Microsystems was acquired by Oracle and this state remains until now (“VirtualBox – Wikipedie,” n.d.).

Virtualbox functionality is to run multiple guest OS's (Operating System) under a single host operating system. Guest operating system acts like it is running on a real hardware with all of its functionality. Virtualbox allows to make snapshot of guest OS. It saves the current state of guest OS and the system can be restored to this state anytime.

5.3 Ubuntu Server 12.04.4 LTS (Long Time Support)

Ubuntu is a Linux based operating system. It is released under GPL license. Development of this distribution is sponsored by Canonical Ltd. Server edition differs from classic edition with absence of X Window environment. 12.04.4 is the version and LTS means long term support. The length of support is 5 years for server edition (“The world’s most popular free OS | Ubuntu,” n.d.).

Linux is an open source software originally developed by Linus Torvalds. Name Linux is derived from Linus and Unix. Linus Torvalds was developing Linux as a hobby during his studies on Helsinki University. He was inspired by Unix and MINIX. Nowadays it is used all around the world mostly as server OS or in HPC (High Performance Computing).

5.4 Honeyd

Honeyd is a small daemon that creates virtual hosts on a network. The hosts can be configured to run arbitrary services, and their personality can be adapted so that they appear to be running certain operating systems. Honeyd enables a single host to claim multiple addresses - tested up to 65536 - on a LAN for network simulation. Honeyd improves cyber security by providing mechanisms for threat detection and assessment. It also deters adversaries by hiding real systems in the middle of virtual systems. (“Honeyd - Network Rhapsody for You,” n.d.).

5.5 Vim

Vim is an advanced, highly configurable text editor. It is released under GPL compatible license - charityware. It is an improved version of UNIX text editor vi. It requires some time to learn how to work with it but then it will make programmers work more efficient. Vim is available on most UNIX-like operating systems. A big advantage is that vim works in terminal so it is very useful for editing files on systems without GUI (Graphic User Interface).

5.6 TeamViewer

TeamViewer is a proprietary software which allows the user to remotely control PC and has many other usages like file sharing and much more. It runs on multiple operating systems and even supports to access a remote machine through a web browser. TeamViewer must be installed on both machines – client and remote host to establish connection.

TeamViewer security is guaranteed by RSA (Rivest, Shamir, Adleman) private/public key exchange (2048-bit) and AES (Advanced Encryption Standard) session encryption (256-bit). In default the software uses servers of teamviewer.com to start connection. In 70 percent of cases is established direct TCP or UDP connection. In other cases connections are routed through TeamViewer GmbH's network (TCP or HTTP-tunneling). In Figure 6 you can see the deployment of TeamView.

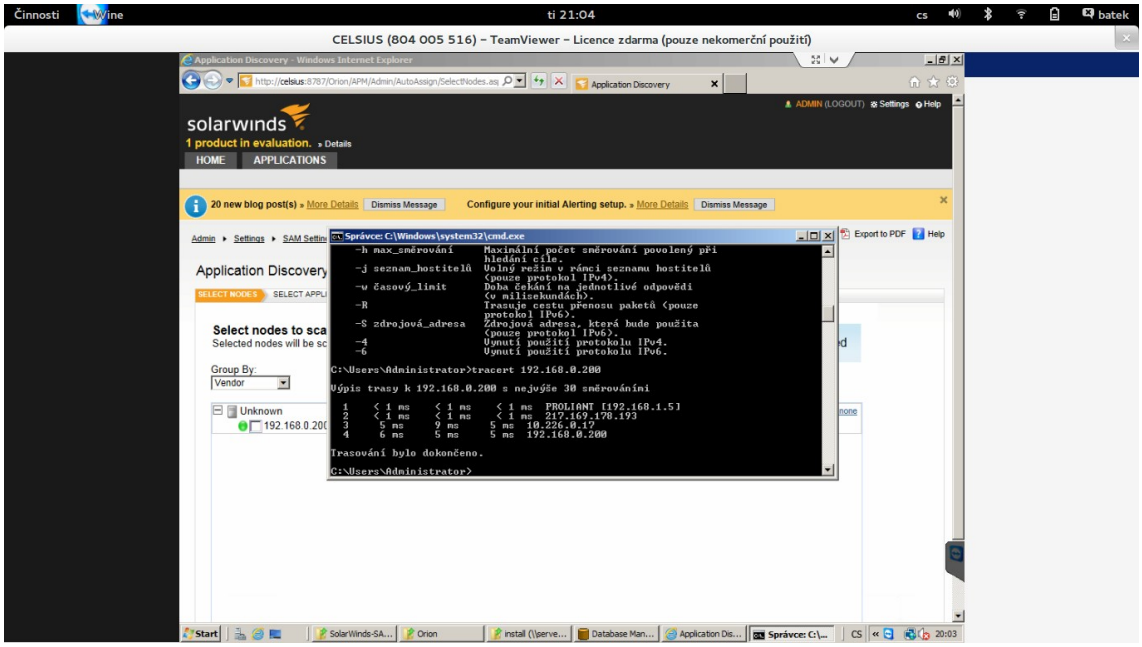

Figure 6. TeamView in use

5.7 BASH

Bash is UNIX shell which creates interpret for command line. It is made by Brian Fox. Its name is an acronym to Bourne again shell.

It is intended to conform to the IEEE (Institute of Electrical and Electronics Engineers) POSIX (Portable Operating System Interface) P1003.2/ISO 9945.2 Shell and Tools standard. It offers functional improvements over sh for both programming and interactive use. In addition, most sh scripts can be run by Bash without modification.

The improvements offered by Bash include:

- Command line editing
- Unlimited size command history
- Job Control
- Shell Functions and Aliases
- Indexed arrays of unlimited size
- Integer arithmetic in any base from two to sixty-four (“Bash - GNU Project - Free Software Foundation,” n.d.)

5.8 Solar winds

Two products from Solar Winds company were used in the work.

5.8.1 Server & Application Monitor

Application Monitoring for all components – servers, virtual layer, and applications such as SQL (Structured Query Language) Server®, Exchange, and Active Directory®

- Easily customize alerts, reports, and dashboards for your enterprise-wide needs
- Use baseline to compare application performance and alert when apps start having issues
- Great value for money – monitoring, reporting, alerting, and asset inventory in one product
- Easy server monitoring software for collaborating across server, Web, database, and application teams (“Server Monitoring & Application Performance Management,” n.d.)

5.8.2 Network Performance Monitor

Simplifies detection, diagnosis, & resolution of network issues before outages occur

- Tracks response time, availability, & uptime of routers, switches, & other SNMP-enabled (Simple Network Management Protocol) devices
- Shows performance statistics in real time via dynamic, drillable network maps
- Automatically discovers SNMP-enabled network devices & typically deploys in less than an hour (“Network Monitoring Software & Discovery Tool | SolarWinds,” n.d.)

6. Solution

To make all the tasks properly theoretical background was needed. Studying Internet protocols and OSI model was necessary to give the best results.

6.1 Documentation

The first thing which the company requested was to create documentation of the network. The request was to make documentation of physical layer only. So basically it meant that documentation had to be made including all network

hardware devices like computers or printers, all UPT sockets in the walls and finally interconnection between all these devices and network hardware.

The first thing that had to do be done was to document the whole network. This task was about exploring all spaces of the company's offices for devices which should be mentioned in the documentation. The output of this task then should be understandable for all people who are involved in networking. In Figure 7 you can see the example of the result. The documentation was designed for reading in landscape mode.

The next task was to design a naming system for UTP sockets. It was because there were not any.

Because every office had a unique number on the doors the idea of the naming was based on this. The naming convection invented is the following – office number modulo 100 + socket number + office number / 100 - 1. So for example if the office number was 103 and there are four sockets, that gives us the results of socket names 31, 32, 33, 34 (103 mod 100 + (1,2,3,4) + 103/100(int) - 1). This naming system design was accepted by company.

The result of documentation was made in Microsoft Visio. There were four floors that had to be documented.

During the process of making documentation of the company's network, some employees noticed that their network connection should be checked. From this situation came the next task. Mainly the task was to analyze the function of all interfaces and packet loss if some exist.

6.2 Network performance

For this task remote server in the company network was assigned. This server was accessed through TeamView remote control software. It was probably a virtual server.

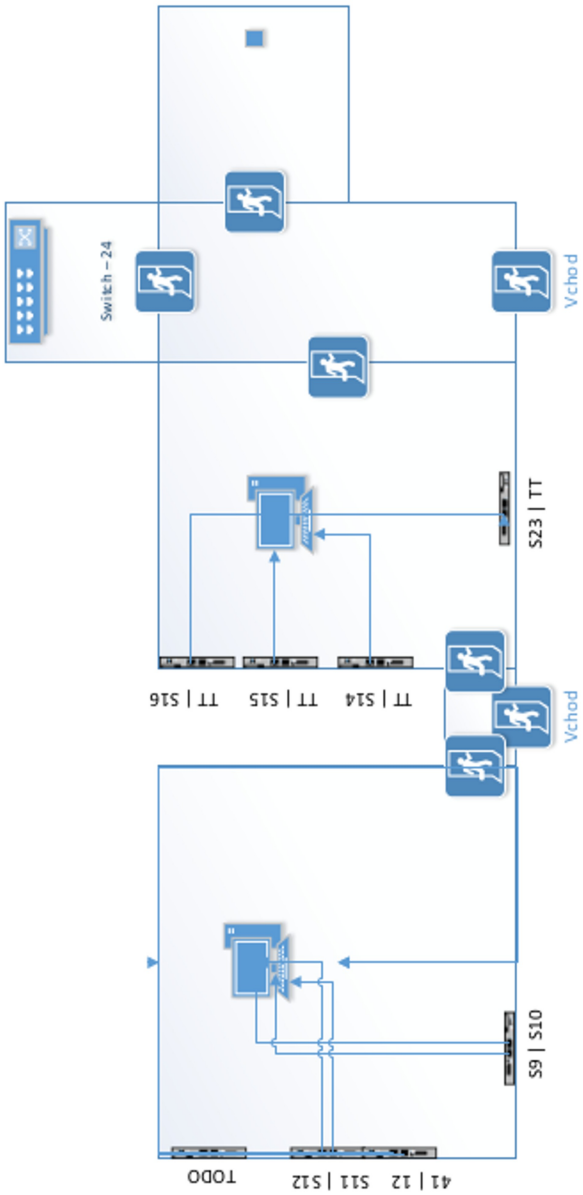

Figure 7. Documentation example

Server hardware:

- Processor: Intel Xenon CPU (Central Processor Unit) 2.4 GHz
- Memory: 3GB
- OS: Microsoft Windows Server Standard

The first thing was to choose an appropriate software for this task. System administrator proposed SolarWinds software for the network analysis. But he had problems with commissioning of the software. So the first job in this task was to get the software working.

After installation the software did not work, even when the company administrator contacted SolarWinds support, the software still was not in operation. After reading a lot of SolarWinds documentation were tried different web browsers – because the software had web GUI and the problem was that login into SolarWinds was impossible.

Because it was the company's server, for any change in serves file system approval by server administrator was needed. The original web browser was Microsoft's Internet Explorer so Mozilla Firefox was tried – and it was working. Even when the official documentation said that Internet Explorer is supported. In Figure 8 you can see SolarWinds in operation.

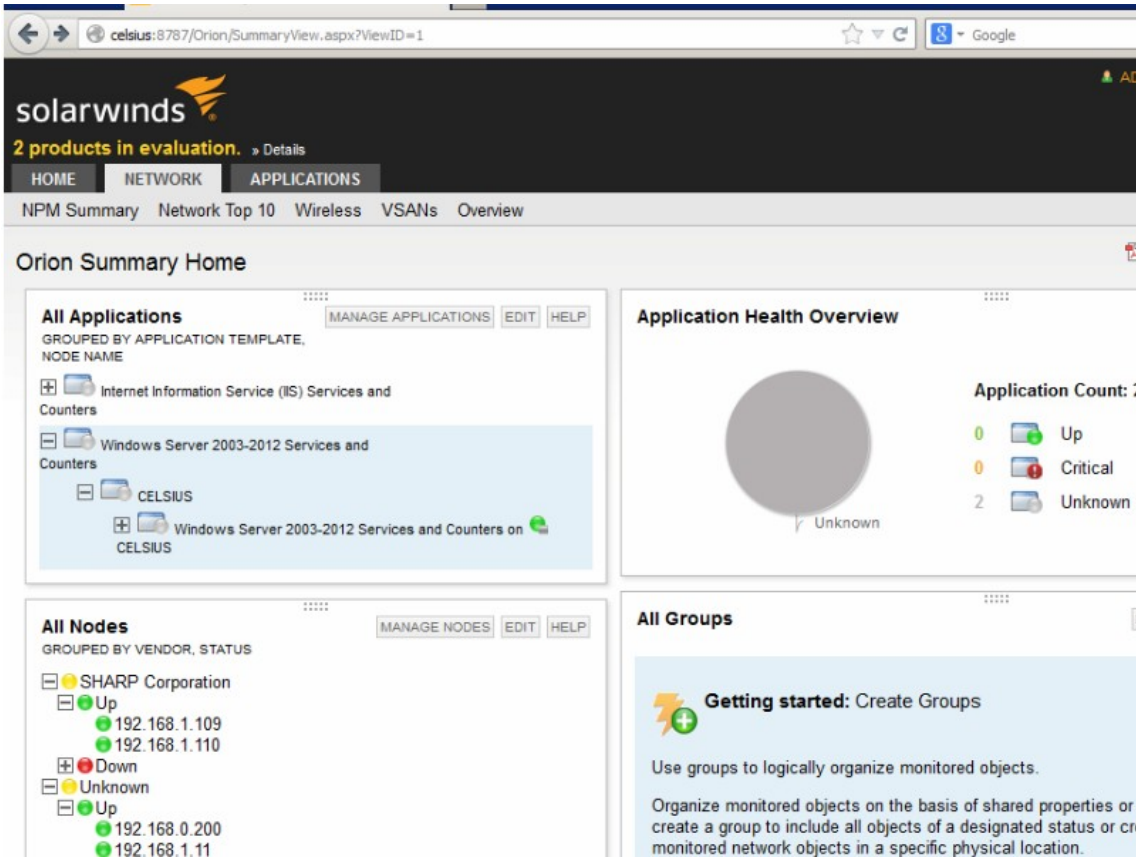

Figure 8. SolarWinds example

The first step to analyze network devices with SolarWinds software is to add them to the software's database. The process is called discovery. It can be made by one by one typing every IP address manually . But a more advanced option was choosen – discovering devices in address range.

Because the company network devices are using private address from range 192.168.0.0/16 and are using only the first two subnets, the discovery was made on this private address range, but with netmask 255.255.254.0. The Solarwinds then tries all addresses in this range an tests them on protocols configured by the user.

This gave the list of the connected devices and their IP addresses. Then the next step was analyzing their interfaces packet loss, bandwidth and so on. The results of the analysis were reported to the network administrator.

The problem was with the UTP sockets to which there were no devices connected. |n this situation there had to be cooperation with the system administrator. He was connecting the device to each unused socket and the author made analysis on the server. In this case every address had to be written manually. In this task we used documentation which was made before and it simplified the analysis.

6.3 Honeypot

The last task was to offer some improvements to the company's network environment. Because the author is interested in computer security it was offered to create a honeypot solution to increase cyber security in the network. The offer was accepted by the company.

The author's first contact with honeypot was in his computer security class at university. He was very interested in this technology. Honeypot refers to a honey pot trap which attracts some animals but they do not realize that it is a trap. In computer security honeypot refers to the same thing to attract hackers as an easy victim. A very simple honeypot could be for example an email address which nobody is using for private mail. From such a mailbox security experts can then analyze mail and obtain spammer's email addresses.

There are two main groups of honeypots:

- high-interaction honeypots
- low-interaction honeypots

High interaction honeypot could be for example a normal Linux machine but with modified kernel. This kind of a honeypot usually uses a weak SSH password to allow the attacker to take control of the system. Then all actions of intruder are logged. This solution is very good in the sense that the attacker does not know that he/she is on honeypot system, but it is very time consuming to take care of such a system and analyze intruder's actions.

Low interaction honeypots are usually only computer programs which are running as daemon. These programs usually simulate simple services, but the intruder cannot take control of them. Of course if there are some vulnerabilities of which we do not know, then the intruder can take control of the system.

Low-interaction honeypot was selectedfor this task, secifically honeyd.

The author got all his knowledge about honeyd from the book by Thorsten Holz and Niels Provos (“Virtual Honeypots: From Botnet Tracking to Intrusion Detection: Niels Provos, Thorsten Holz: 9780321336323: Amazon.com: Books,” n.d.). The book name is Virtual Honeypots: From Botnet Tracking to Intrusion Detection . This book contains all information necessary to deploy honeyd.

Honeyd is configured by configuration files. The syntax of these files is a context-free grammar. If there is more than one host to be deployed then the system is called honeynet.

The honeyd is a computer program. It runs on UNIX based and Windows operating systems. But Windows version might not include all functionality provided on Linux systems. So for the solution Linux-based operating system – Ubuntu 12.04 LTS server was selected. This system does not include GUI, because on server it is just wasting with rescources.

Ubuntu includes honeyd package in its repositories, but it is not the latest version. The original authors stopped supporting it in 2007. But development

continued in project Nova. For this task this implementation was used. It is only a source code on GitHub so honeyd had to be compiled first.

Problems

As mentioned Ubuntu server was used as the operating system. The system runs in Virtualbox as a virtual OS. It is because the solution was designed to run in the company on a virtual machine too.

But in virtualox all devices are not acting as real hardware. The biggest problem was to make honeyd work on network with author's laptop for testing purposes. Firstly honeyd was deployed on loopback interface, which was working normally. But on Ethernet interface in virtualbox the system does not react to incoming packets. A lot of time trying different configurations was consumed, because there is no documentation to this behavior. Then it was discovered that virtualbox does not allow promiscuous mode by default.

Normally the network interface card passes to the system only data with appropriate MAC (Media Access Control Address) address (OSI layer 2) and drops others. But in promiscuous mode system can see all data on the network card. And honeyd uses this technique to fool ARP (Address Resolution Protocol) protocol so it is essential for proper function. It took some time before the author found out that he had to switch the virtualbox network card to this mode which works normally on real hardware. After that everything worked perfectly.

When request comes to MAC address the network interface card sends this information to OS and honeyd responds with its own IP address. As we can see in Figure 9, where one simple honeypot is made in debug mode so we can see debug information, the honeyd requested IP address from DHCP (Dynamic Host Configuration Protocol) server and then the updated ARP protocol binding. At this moment other devices on the network think that there is a new device with IP address 192.168.0.173.

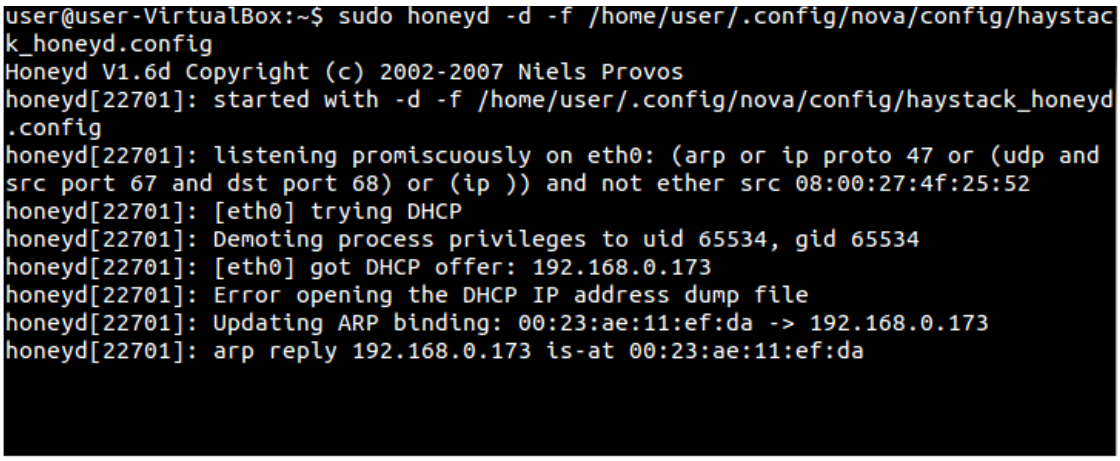

Figure 9. Example of starting honeyd

For honeyd to act as a real system it is necessary to simulate common services like web server and such. These services are usually written in Python or BASH, but other languages are supported too. The services than act as their real world models but obviously do not provide the same functionality. Basically we can read data from STDIN and the respond to STDOUT which means incoming respectively outgoing network traffic.

Example of simple BASH script:

```
#!/bin/sh
   # Test script for Honeyd
   DATE=`date`
   LOGDIR=/var/log/honeypot/
   [ ! -e "$LOGDIR" ] && LOGDIR=/tmp
   LOGFILE=$LOGDIR/log_test
   echo "$DATE: Started From $1 Port $2" >> $LOGFILE
   echo SSH-1.5-2.40
   while read name
   do
      echo "$name" >> $LOGFILE
         echo "$name"
   done
```

Honeypot is designed mainly for catching traffic which should be close to zero, because it is not a real system. From this traffic we can guess that somebody is trying to break our network integrity, is sending Spam or some auto scan bots are present in our network – which means that there is some PC infected.

Here is an example of one line from the logfile, from which we can guess that somebody is trying to connect to telnet:

- **honeyd[3482]: E(192.168.0.194:33728 - 192.168.0.175:23): Attempted login: admin/admin**

From this example we can see that there is a logged attacker IP address, honeypot address both port numbers and data which was sent. This example used a script to emulate telnet which is included in default honeyd installation.

The final solution for the deployment to the company contained a virtual disk image. In this virtual disk Ubuntu 12.04 server edition was installed, compiled with the latest version of honeyd. And honeyd was configured with honeynet, which fits to the company network environment which was explored earlier.

7. Summary

During the work I gained very useful information about network environment in a real company. Very valuable for me are the skills which I gained during meetings in the company, because it was my first working experience in information technology area.

I learned how to solve real problems which occurred during my practice in an efficient way. Also communication with real IT professionals increased my ability to work in a team of IT specialists.

I came into contact with very interesting software which I had not even known before like SolarWinds or remote connection through TeamView. I also learned a lot of useful information during preparation of honeyd in cyber security area, which I am very interested in and I would like to focus my interest on this area in the future.

Working for MPS company was a great experience with a lot of useful information about the technology from IT area.

8. References

Address Resolution Protocol - Wikipedia, the free encyclopedia [WWW Document], n.d. URL http://en.wikipedia.org/wiki/Arp_protocol (accessed 4.16.14).

Bash - GNU Project - Free Software Foundation [WWW Document], n.d. URL https://www.gnu.org/software/bash/ (accessed 4.15.14b).

Company | MPS Mont a.s. [WWW Document], n.d. URL http://www.mps-mont.cz/en/Company.html (accessed 4.15.14).

Cyclic redundancy check - Wikipedia, the free encyclopedia [WWW Document], n.d. URL http://en.wikipedia.org/wiki/Cyclic_redundancy_check (accessed 4.16.14).

Data link layer - Wikipedia, the free encyclopedia [WWW Document], n.d. URL http://en.wikipedia.org/wiki/Data_link_layer (accessed 4.15.14b).

Domain Name System - Wikipedia, the free encyclopedia [WWW Document], n.d. URL http://en.wikipedia.org/wiki/Dns (accessed 4.16.14).

Dynamic Host Configuration Protocol - Wikipedia, the free encyclopedia [WWW Document], n.d. URL http://en.wikipedia.org/wiki/Dhcp (accessed 4.16.14).

File Transfer Protocol - Wikipedia, the free encyclopedia [WWW Document], n.d. URL http://en.wikipedia.org/wiki/Ftp (accessed 4.16.14).

GNU General Public License - Wikipedia, the free encyclopedia [WWW Document], n.d. URL http://en.wikipedia.org/wiki/GNU_General_Public_License (accessed 4.16.14).

Honeyd - Network Rhapsody for You [WWW Document], n.d. URL http://www.citi.umich.edu/u/provos/honeyd/ (accessed 4.15.14b).

International Organization for Standardization - Wikipedia, the free encyclopedia [WWW Document], n.d. URL http://en.wikipedia.org/wiki/Iso (accessed 4.16.14).

Internet Protocol - Wikipedia, the free encyclopedia [WWW Document], n.d. URL http://en.wikipedia.org/wiki/Internet_Protocol (accessed 4.16.14).

MAC address - Wikipedia, the free encyclopedia [WWW Document], n.d. URL http://en.wikipedia.org/wiki/Mac_address (accessed 4.16.14).

Network layer - Wikipedia, the free encyclopedia [WWW Document], n.d. URL http://en.wikipedia.org/wiki/Network_layer (accessed 4.15.14b).

Network Monitoring Software & Discovery Tool | SolarWinds [WWW Document], n.d. URL http://www.solarwinds.com/network-performance-monitor.aspx (accessed 4.15.14b).

OSI model - Wikipedia, the free encyclopedia [WWW Document], n.d. URL http://en.wikipedia.org/wiki/OSI_model (accessed 4.15.14).

Physical layer - Wikipedia, the free encyclopedia [WWW Document], n.d. URL http://en.wikipedia.org/wiki/Physical_layer (accessed 4.15.14b).

Port (computer networking) - Wikipedia, the free encyclopedia [WWW Document], n.d. URL http://en.wikipedia.org/wiki/Port_number (accessed 4.15.14b).

Protocol data unit - Wikipedia, the free encyclopedia [WWW Document], n.d. URL http://en.wikipedia.org/wiki/Protocol_data_unit (accessed 4.15.14).

Server Monitoring & Application Performance Management [WWW Document], n.d. URL http://www.solarwinds.com/server-application-monitor.aspx (accessed 4.15.14b).

Simple Network Management Protocol - Wikipedia, the free encyclopedia [WWW Document], n.d. URL http://en.wikipedia.org/wiki/Snmp (accessed 4.16.14).

SQL - Wikipedia, the free encyclopedia [WWW Document], n.d. URL http://en.wikipedia.org/wiki/Sql (accessed 4.16.14).

The world’s most popular free OS | Ubuntu [WWW Document], n.d. URL http://www.ubuntu.com/ (accessed 4.15.14b).

Transmission Control Protocol - Wikipedia, the free encyclopedia [WWW Document], n.d. URL http://en.wikipedia.org/wiki/Transmission_Control_Protocol (accessed 4.15.14).

Transport layer - Wikipedia, the free encyclopedia [WWW Document], n.d. URL http://en.wikipedia.org/wiki/Transport_layer (accessed 4.15.14b).

UDP - Wikipedia, the free encyclopedia [WWW Document], n.d. URL http://en.wikipedia.org/wiki/Udp (accessed 4.15.14b).

VirtualBox – Wikipedie [WWW Document], n.d. URL http://cs.wikipedia.org/wiki/VirtualBox (accessed 4.15.14b).

Virtual Honeypots: From Botnet Tracking to Intrusion Detection: Niels Provos, Thorsten Holz: 9780321336323: Amazon.com: Books [WWW Document], n.d. URL http://www.amazon.com/Virtual-Honeypots-Tracking-Intrusion-Detection/dp/0321336321 (accessed 4.15.14b).